connect MT
Verbund für medizinische Telekooperationen

JiveX

VISUS

System-voraussetzungen

DICOM-Mail Gateway in connectMT
(ehem. Westdeutscher Teleradiologieverbund)
Stand 02 | 2024

VISUS Health IT GmbH
Gesundheitscampus-Süd 15
D-44801 Bochum

t +49 (234) 93693-200
support@visus.com

www.visus.com

Inhaltsverzeichnis

Inhaltsverzeichnis 2
Einleitung 3
Systemanforderungen Server 3
Unterstützte Betriebssysteme 3
Serverausstattung (empfohlene Voraussetzungen bei intensiver Nutzung) 3
Systemsicherheit 3
Systembetrieb 3
Softwarebackup 4
Virenscanner 4
Firewall-Regeln 5
Datenversand 5
JiveX Status Monitoring 5
Verwendete Clients 5
VPN-Zugang 6

Einleitung

Dieses Dokument enthält die Systemvoraussetzungen für DICOM-Mail Gateways in connectMT. Die genannten Anforderungen gelten gleichermaßen für virtualisierte als auch physische Systeme.

VISUS betreibt und stellt die Software für die Realisierung der technischen Infrastruktur für das Netzwerk connectMT der MedEcon Telemedizin GmbH bereit. Hierbei wird die eigenentwickelte Software JiveX als DICOM-Mail Gateway in der Infrastruktur des Kunden betrieben.

Systemanforderungen Server

Unterstützte Betriebssysteme

Es werden folgende Betriebssysteme im jeweils aktuellen Patchlevel unterstützt:

- Microsoft Windows 10 64bit
- Microsoft Windows 11 64bit
- Microsoft Windows Server 2016/ 2019
- Microsoft Windows Server 2022

Die Einrichtung und Partitionierung der Systempartitionen erfolgt nach Best-Practice Vorgaben des Kunden. JiveX nutzt ausschließlich u. g. Partitionen D:\ und E:\ zur Installation und Dateiablage.

Serverausstattung (empfohlene Voraussetzungen bei intensiver Nutzung)

- 8 CPU-Kerne
- 24 GB RAM
- C: Partition für Betriebssystem nach Kundenvorgabe
- Zusätzlich min. 250 GB Speicherplatz aufgeteilt in D: 50 GB und E: 200GB

Systemsicherheit

Systembetrieb
Die insgesamt zunehmende Bedrohungslage durch Schadsoftware erfordert grundsätzlich, dass die bekannten Vorkehrungen für den sicheren Betrieb des DICOM-Mail Gateways getroffen werden. Im Besonderen wird auf die nachfolgenden Maßnahmen hingewiesen:

- VISUS empfiehlt den Betrieb des Systems in einer möglichst vom übrigen Netzwerk (intern/extern) separierten Umgebung. Es sollten nur die für den Betrieb notwendigen Ports zum Betrieb geöffnet sein. Die Ports sind abhängig von ihrer individuellen Installation und müssen daher bei Einrichtung mit dem zuständigen VISUS-Mitarbeiter abgesprochen werden.
- Es ist davon abzusehen, dass dauerhaft Laufwerksfreigaben auf das Gateway eingerichtet werden. In der Regel ist dies für den Betrieb des Gateways nicht erforderlich.

- Windows Systemupdates/-upgrades sollten bei Verfügbarkeit möglichst direkt eingespielt werden. Eine automatisierte Überwachung dieses Prozesses wird empfohlen.

Softwarebackup
Um eine schnelle und reibungslose Wiederherstellung des DICOM-Mail Gateways bei Server- bzw. Systemfehlern zu gewährleisten, werden Backups der Konfigurations- und Datenbanktabellen auf dem DICOM-Mail Gateway abgelegt.
Diese werden mithilfe einer geplanten Aufgabe jede Nacht automatisch unter E:\backup gesichert und 5 Tage aufbewahrt.

Wir möchten Sie bitten diese Backups zusätzlich auf einem anderen Speicher zu sichern, damit wir bei einem Serverausfall oder defekten Platten das DICOM-Mail Gateway möglichst schnell wiederherstellen können.

Virenscanner
Zur weiteren Absicherung empfehlen wir den Einsatz eines Virenscanners. Erfahrungsgemäß läuft JiveX mit den gängigen Produkten einwandfrei. Die Verwendung eines Virenscanners kann jedoch großen Einfluss auf die Systemperformance haben.
Um einen optimalen Betrieb zu ermöglichen, empfehlen wir daher folgende Ordner und Prozesse als Ausnahmen zu definieren:

1. Die Ordner in denen sich die Bild- / Dokumentendaten befinden (`D:\VISUS\jivexcs\images` und Unterordner bzw. angebundene Laufwerke)
2. Die Ordner `D:\VISUS\` und `D:\mariaDB\data`
3. Folgende Prozesse:
   - %JCS_HOME%\bin\CSNTService.exe
   - D:\VISUS\MariaDB\bin\mysqld.exe
   - %JCS_HOME%\bin\tools\rtf2pdf\rtf2pdf.exe
   - %JCS_HOME%\bin\tool\PDFMaker\VTPDFMaker.exe

Sollte es nicht möglich sein, ganze Ordner als Ausnahmen zu definieren, können Sie alternativ auch die folgenden Dateitypen als Ausnahme definieren:
- .dicom
- .dicomzip
- .dcmpre
- .pre
- .jp2
- .jp5
- .dcmjp2k
- .dcmjp2kl

Firewall-Regeln

Datenversand
Der Datenversand erfolgt über Mailserver, die von VISUS betrieben werden. Sämtlicher Datenverkehr ist dabei zertifikatbasiert SSL-verschlüsselt. Die Authentifizierung an den Mailservern erfolgt ebenfalls über von VISUS herausgegebene SSL-Zertifikate.
Für den korrekten Betrieb ist daher die ausgehende Kommunikation zu folgenden Servern über die TCP-Ports 25 (SMTP/TLS) und Port 995 (POP3S) sicher zu stellen. Der Einsatz von Proxyserver oder Firewalls, die eigene SSL-Zertifikate nutzen, um den Datenverkehr zu scannen, ist aufgrund der eingesetzten SSL-Authentifizierung nicht möglich.

- mail1.dicommail.com
- mail2.dicommail.com
- mail3.dicommail.com
- mail4.dicommail.com
- mail5.dicommail.com
- mail6.dicommail.com

JiveX Status Monitoring
VISUS nutzt zur Überwachung des Betriebszustandes und zur Administration der JiveX-Dienste ein Monitoring auf Basis der Software *check_mk*. Die Freischaltung dieses Monitoring-Dienstes ist grundlegender Teil der getroffenen Servicevereinbarung im Rahmen der Teilnahme im Netzwerk connectMT und daher essenziell. Nur durch den konsequenten Einsatz und die Überwachung von Statusinformationen kann der Betrieb der Verbundstruktur nachhaltig sichergestellt werden.
Im Rahmen des Monitorings werden weder personenbezogene Daten wie Benutzerzugänge noch Patientendaten verarbeitet oder gespeichert. Sämtliche Kommunikation erfolgt verschlüsselt und wird durch zertifikatbasierte Authentifizierungsmechanismen geschützt. Details zu dieser Lösung senden wir Ihnen gerne auf Anfrage zu.
Zur Einrichtung wird eine weitere Firewall-Freischaltung für die ausgehende Kommunikation zu dem von VISUS betriebenen Monitoring-Server benötigt:

- atlas79.mydhp.de Port 8140 [TCP]

Verwendete Clients

Als Client steht mit JiveX Web ein HTML5-basierter Zero-Footprint Webclient zur Verfügung. Dieser Client ist lauffähig und freigegeben für alle gängigen Browser unter Windows und MacOS. Detaillierte Freigabelisten stellen wir auf Anfrage gerne zur Verfügung.
Als Systemressourcen werden ca. 500 MB Arbeitsspeicher, abhängig vom anzuzeigenden Datenvolumen, am Client benötigt.

VPN-Zugang

Für Installation und Wartung ist ein Fernwartungszugang zum Mailgateway erforderlich, der durch den Kunden bereitzustellen ist. Es stehen folgende Verbindungsarten zur Verfügung:

- IP/SEC Site2Site Verbindung
    - Dieses Verfahren hat für Sie den Vorteil, dass Sie vor jeder VPN-Verbindung eine automatische E-Mail erhalten.
- Installation des SecureLink Clients auf den TRV-Server. Dieser baut eine verschlüsselte Verbindung zu unserem Securelink-Server auf.
    - Dieses Verfahren hat für Sie den Vorteil, dass Sie vor jeder VPN-Verbindung eine automatische E-Mail erhalten.
- CGM Anydesk. Diese Version ist nicht kompatibel zu der freien Anydesk Version. Nur Mitarbeiter von der CGM oder Visus können eine Verbindung aufbauen. Es gibt dabei 2 unterschiedliche Versionen. Bei einer Version müssen Sie jede Verbindung mit Mausklick einzeln bestätigen. Bei der anderen Version gibt es zu der Anydesk-Nr. (ähnlich TeamViewer) ebenfalls noch ein Passwort.